PRIVACY IMPACT ASSESSMENT

electronic Document Processing (eDP)

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Name of system: electronic Document Processing (eDP)
(b) Bureau: Consular Affairs (CA)
(c) System acronym: eDP
(d) iMatrix Asset ID Number: 5091
(e) Reason for performing PIA: Click here to enter text.

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

eDP is currently undergoing its Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. The estimated ATO date is Summer 2021.

(c) Describe the purpose of the system:

The electronic Data Processing (eDP) system provides National Visa Center (NVC) users capabilities to electronically upload immigrant visa (IV) support documents and paper-based files received for storage and retrieval. Documentation scanned or uploaded via the eDP system at the NVC is replicated to the Consular Consolidated Database (CCD) at frequent intervals to allow posts to view supporting documentation. Information is also replicated from the CCD to eDP from applications submitted by applicants via the Consular Electronic Application Center (CEAC) system. The eDP system allows NVC users to scan, view, and edit immigrant visa documentation received at the NVC. The eDP mission requirements supporting the Bureau of Consular Affairs (CA) are as follows:

- To receive immigrant visa supporting documents in electronic form and store them in the Consular Consolidated Database (CCD) so that posts and external agencies can access them. Immigrant Visa Information System (IVIS) users create a bin/text file of data for case processing at posts. Users attach these bin files via the eDP system to store them in the eDP database which will also be replicated to CCD.

- To provide an interface to scan the paper files received at the NVC and store them electronically for access by NVC staff to conduct visa processing.

eDP uploads documents which are hosted on its database and replicated and stored in the CCD. The eDP web components (eDP Web Central and eDP Web Post) allow users to access CCD at posts and external agencies such as the Department of Homeland Security (DHS) to view the immigrant visa (IV) documents related to IV cases. Users are able to retrieve and view documents associated with a case or an applicant in a printable report format. eDP Web Central is hosted on and accessed from the CCD allowing eDP users to view and print documents. eDP Web Post can be accessed from the Immigrant Visa Information System (IVIS) Immigration Visa Overseas (IVO) application tables or as a menu item in the local post CCD database allowing NVC users to print information. CCD, IVIS and CEAC systems are outside the boundary of the eDP system.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

eDP contains the following information on U.S. citizens (family members of the non- U.S. citizen immigrant visa applicants): name, birthdate, phone number, business and personal address, email address, images or photos.

Non-U.S. Citizen (immigrant visa applicants) PII: name, citizenship, birthdate, place of birth, phone number, personal address, email, legal information, employment information, aliases, images, passport photo, social security number (SSN), and passport and national ID numbers.

eDP also collects business information on company/employer name, location, address, email address, and job title for both U.S. citizens and non-U.S. citizens.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. §§ 1151-1363a (Title II of the Immigration and Nationality Act of 1952, as amended);
- 8 C.F.R. § 245.1(a);
- 8 U.S.C. § 1104 (Powers and Duties of the Secretary of State);
- 22 U.S.C. § 2651a (Organization of the Department of State);
- 22 C.F.R. Parts 40-42, and 46 (Visas);
- 26 U.S.C. § 6039E (Information Concerning Resident Status);
- Immigration Act of 1990, PL 101-649, November 29, 1990 (an Act to amend the Immigration and Nationality Act of 1952);
- Illegal Immigration Reform and Immigration Responsibility Act of 1996, PL 104-208, Div. C, September 30, 1996;
- Omnibus Consolidated Appropriations Act, 1997, PL 104-208, September 30, 1996;

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

☒Yes, provide:
- SORN Name and Number: Visa Records – STATE-39
- SORN publication date: June 15, 2018

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No

If yes provide:
- Schedule number Department of State Records Disposition Schedule:

A-14-001 Visa Records, B-09-001 and 002 Consular Records

A-14-001-002a*:* Visa Case Files on Individual Aliens
Description: Case files on individual aliens issued an immigrant visa.
Disposition: Destroy 6 months after issuance.
DispAuthNumber: N1-059-86-02, item 1a

A-14-001-002b: Visa Case Files on Individual Aliens
Description: Case files on individual aliens issued a non-immigrant visa
Disposition: Destroy 1 year after issuance.
DispAuthNumber: N1-059-86-02, item 2b

A-14-001-02c(1)(a): Visa Case Files on Individual Aliens
Description: Case files on individual aliens refused a visa. (1) Cases of living visa applicants. (a) Cases of applicants refused or presumed ineligible on the basis of Sections 212(a) (1), (2), (3), (4), (5), (9), (10), (12), (13), (19), (22), (23), (27), (28), (29), (31), and (34) of the Immigration and Nationality Act.
Disposition: Retain until alien is 90 years of age or older, provide there has been no visa activity for the past 10 years, at which time destroy. (ref. NC1-59-86-2, item 3c1(a) and c1(c)).
DispAuthNumber: N1-059-91-28, item 1c(1)).

A-14-001-02c(1)(b): Visa Case Files on Individual Aliens
Description: Cases of applicants refused or presumed ineligible under Section 212(a)(33) of the Immigration and Nationality Act.
Disposition: Retain until alien is 100 years of age, then destroy. (ref. NC1-59-86-2, item 2c1(b))

DispAuthNumber: N1-059-91-17, item 1

A-14-001-02c(1)(c): Visa Case Files on Individual Aliens
Description: Case files on individual aliens refused a visa. (1) Cases of living visa applicants. (c) Cases of applicants refused or presumed ineligible under all other Sections of Section 212(a), (Category II), and Section 212(e) of the Immigration and Nationality Act.
Disposition: Destroy 2 years after date of refusal.
DispAuthNumber: N1-059-86-02, item 6d

A-14-001-02c(1)(d): Visa Case Files on Individual Aliens
Description: Case files on individual aliens refused a visa. (1) Cases of living visa applicants. (d) Cases of applicants refused or presumed ineligible on the basis of Section 212(a) (17) of the Immigration and Nationality Act.
Disposition: Retain for 20 years, then destroy. (ref. N1-059-86-2, item 7)
DispAuthNumber: N1-059-91-28, item 1c(1)(d)

A-14-001-02c(1)(e) Visa Case Files on Individual Aliens
Description: Case files on individual aliens refused a visa. (1) Cases of living visa applicants. (e) Cases of applicants refused or presumed ineligible on the basis of Sections 212(a)(1)(A)(ii), (1)(A)(iii), (2), (3)(A), (3)(B), (3)(C), (3)(D), (3)(E)(ii), (6)(C), (6)(E), (6)(F), (8) and (9)(C) of the Immigration and Nationality Act as of June 1, 1991.
Disposition: Retain until alien is 90 years of age or older and there has been no visa activity for the past 10 years, at which time destroy.
DispAuthNumber: N1-059-92-05, item 1c(1)(e)

A-14-001-02c(1)(f): Visa Case Files on Individual Aliens
Description: Case files on individual aliens refused a visa. (1) Cases of living visa applicants. (f) Cases of applicants refused under Section 221(g) of the Immigration and Nationality Act.
Disposition: Destroy 1 year after date of refusal.
DispAuthNumber: N1-059-86-02, item 8c(1)(f)

A-14-001-02c(1)(g): Visa Case Files on Individual Aliens
Description: Cases of applicants refused or presumed ineligible on the basis of Section 212(a)(6) of the Immigration and Nationality Act.
Disposition: Destroy when 15 years old, except where review by consular officer indicates need for further reference value. (ref. NC1-59-86-2, item 5 and N1-059-91-28)
DispAuthNumber: N1-059-88-38, item 1

A-14-001-02c(1)(h): Visa Case Files on Individual Aliens
Description: Case files on individual aliens refused a visa. (1) Cases of living visa applicants. (h) Cases of applicants refused or presumed ineligible on the basis of Section 212(a)(3)(E)(i) of the Immigration and Nationality Act as of June 1, 1991.
Disposition: Retain until alien is 100 years of age, then destroy.
DispAuthNumber: N1-059-92-05, item 1c(1)(h)

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?

8 USC§§1101-1503 (see §§ 1104, 1154, 1185 and 1202(a) and (b)); Title II of the Immigration and Nationality Act of 1952, as amended

(c) How is the information collected?

Forms and documents submitted by the IV applicant, petitioner, or legal representative are sent to the NVC either via mail or via electronic transfer from the CEAC system. Hard copy documents are scanned or uploaded into the eDP system via an eDP client workstation application. Once information is collected via the eDP system, the information can be viewed via the eDP Web.

Information from the following forms are captured in eDP, which may contain PII:

DS-0234, Special Immigrant Visa Biodata Form
DS-157, Supplemental Special Immigrant Visa Chief of Missions Application
DSP-122, Supplemental Registration for the Diversity Immigrant Visa Program
I-797, Notice of Action
I-864, Affidavit of Support under Section 213A of the INA
I-864A, Contract between Sponsor and Household Member
I-864EZ, Affidavit of Support under Section 213A of the INA
I-864W Request for Exemption for Intending Immigrant's Affidavit of Support
I-130, Petition for Alien Relative
I-800 Petition to Classify Convention Adoptee as an Immediate Relative
I-526 Immigrant Petition by Alien Entrepreneur
I-129F Petition for Alien Fiancé/Spouse
I-600 Petition to Classify Orphan as an Immediate Relative
I-730 Refugee/AsyleeRelative Petition
I-360 Petition for Amerasian, Widow(er), or Special Immigrant
I-929 Petition for Qualifying Family Member of a U-1 Nonimmigrant
I-140 Immigrant Petition for Alien Worker
I-600A Application for Advance Processing of an Orphan Petition
I-824 Application for Action on an Approved Application or Petition

(d) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
-If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?

Accuracy of the information is the responsibility of the applicant at the point of submission via the source system. Any errors or omissions detected during the IV application review process are called to the attention of the applicant via email or letter.

After documents are uploaded into the eDP system, an accuracy check is performed to ensure the documents are correctly entered.After comparing and verifying the electronic documents against the originals obtained, an eDP Web user who is designated as an Immigrant Visa Overseas Foreign Service Officer (IVO/FSO) then marks the electronic document as "Original Seen and Compared."

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Since the eDP system is not a public-facing system, currency is maintained when the applicant submits an updated application via the source system,which replicates the data in the eDP or when paper-based information received at the NVC is uploaded in the eDP system.

(g) Does the system use information from commercial sources? Is the information publicly available?

The eDP system does not use commercial or publicly-available information.

(h) Is notice provided to the individual prior to the collection of his or her information?

Although the eDP system processes documents that have citizen data and are subject to the Privacy Act and non-citizen data that are subject to INA 222(f), the eDP system is not public-facing. The data are provided to the eDP system via electronic download from DHS or CEAC systems. Notification would be part of the CEAC or DHS systems which are outside the scope of the eDP system.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

The eDP system is not accessed by the public; rather, information is entered into the eDP system from forms the applicant completes via other sources where consent is provided prior to submission to the NVC.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items collected by the eDP system in paragraph 3(d) are essential for verifying identity and/or other elements of applications, but do not extend beyond the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the eDP system to perform the functions for which it is intended.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the PII in the eDP system is to support the State Department's Visa Program. The PII in eDP is used for the processing of IV applications. By digitizing applications and supporting documents, eDP facilitates access to case documents needed for processing actions.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the eDP system provides access to visa information of applicants to support the processing and decisions of immigrant visa cases.

(c) Does the system analyze the information stored in it?

☐Yes
☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information:

The term "internal sharing" traditionally refers to the sharing of information with the Department of State (DoS), but external to the owning organization (referred to as "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures instituted in place within the bureau to protect Sensitive but Unclassified information.

With that understanding, information in the eDP system is shared internally with the CA systems CCD, IVIS, and CEAC as mentioned previously.

Externally, the eDP system information is disclosed to the Department of Homeland Security via the CCD, and may be disclosed to other external Federal agencies such as Treasury and the Social Security Administration consistent with INA 222(f) (8 U.S.C. § 1202(f) visa record confidentiality. Information may also be disclosed to attorneys or petitioners representing an individual in the visa decision making process via email or by U.S. Mail regarding a case.

(b) What information will be shared?

All of the PII listed in section 3(d) is shared both internally and externally. Additionally, the eDP system scans of supporting documents and/or bin files are uploaded at NVC and replicated to CCD to allow posts and external agencies to view the supporting documentation.

(c) What is the purpose for sharing the information?

The purpose of sharing the eDP system PII is to assist NVC case workers and external federal agencies, via CCD, in the processing of visa services.

(d) The information to be shared is transmitted or disclosed by what methods?

The information is shared by secured internal connections with other consular systems (CCD, CEAC and IVIS) and email. All of these activities and systems reside on the Department's secure intranet network, OpenNet. Information shared externally is exchanged through the CCD and utilizes connection-encrypted security technologies.

The eDP system is not interconnected with external offices or agencies. Information is shared via other means, e.g., via the CCD and other CA systems mentioned in paragraph (6a), that are outside the boundary of eDP system.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal Sharing: Numerous management, operational, and technical controls are in place to reduce and mitigate the risks associated with internal sharing of information and disclosure including, but not limited to, annual security training, separation of duties, least privilege assignments and personnel screening.

Safeguards in place for internal sharing also include secure transmission methods (Transmission Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP)) approved by State Department policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures

External sharing: Memorandums of Understanding (MOU/MOA) are in place with other government agencies regarding the handling and use of information, consistent with INA § 222(f) visa record confidentiality.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information in these systems focuses on two primary sources of risk:

Accidental disclosure of information to unauthorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

Deliberate disclosure/theft of information to unauthorized parties regardless whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, other "Sensitive but Unclassified information", and all higher levels of classified information. Users must also sign a user agreement prior to accessing the system.

- Strict role based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level.

- System authorization and accreditation process along with continuous monitoring via a Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared with external agencies via CCD are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals do not have direct access to their information contained in the eDP system; however, procedures on how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record are published in the System of Records Notice (SORN) Visa Records STATE-39 and in rules published at 22 CFR 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.
Individuals cannot correct information in the eDP system directly. However, information can be corrected through correspondence with the overseas post and at the formal interview for the visa. The updated information is either provided electronically or in paper form to the NVC for upload to the eDV.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals are notified of the procedures to correct records in these systems by a variety of methods:

1. During their visa interview
2. Published SORNs

3. Instructions on forms and web pages where applicants complete forms
4. Notifying the Department of State by email or letter that a correction is needed

Each method contains both procedures and contact information.

8. Security Controls

(a) How is the information in the system secured?

The eDP system is secured within the Department of State internal network where risks are mitigated through the use of defense in-depth layers of security, including management, operational, and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties. All physical records containing PII are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only.

Access to eDP applications is controlled at the application level. All accounts/access must be approved by the user's supervisor and the local Information System Security Officer. Each user is required to enter a unique user identifier and password prior to accessing the eDP system and performing any actions. The audit vault is used to monitor all privileged accesses to the system. Data shared with other government agencies are carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officials of each agency.

The eDP system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Each authorized eDP system user must be approved by the supervisor and agree to the user access agreement/rules of behavior before being given an OpenNet user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access. Additionally, each user is assigned a unique user identifier and password for logon to eDP specifically.

Access to the eDP system is role-based and requires managerial concurrence. Access control lists (ACLs) permit only specific categories of information to be accessed by individuals. Local Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The CA System Manager and CA ISSO, in conjunction with the CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides. They also conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, eDP system auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges, or changes in file access restrictions.

The purpose of the eDP system audit trail is to document modification or unauthorized access to the system and to dynamically audit retrieval access to critical data.

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially. The State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational, and technical controls are in place in accordance with NIST and Department of State Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit are encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access or data manipulation. Access to the eDP systems require dual

factor authentication utilizing PIV/CAC and PIN, in addition to a unique user identifier and password for logon.

(f) How were the security measures above influenced by the type of information collected?

Exposure of an individual's PII may lead to inconvenience, distress, or damage to standing or reputation, financial loss, harm to State Department or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation. The security measures listed above in paragraphs (8a-e) are implemented to secure the data in the eDP system in accordance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

eDP post consular officers/users, eDP web users, system administrators, and database administrators have access to data in the system. eDP authorized users include both government and contract employees. The following are the roles:

eDP post consular officers/users: Scan and upload documents into eDP.
eDP web users: Access information to conduct visa processing operations.
System Administrators: Conduct daily maintenance, establish eDP access control lists (ACLs), and backups.
Database Administrators: Conduct daily maintenance, upgrades, patch/hot fixes, backups and configuration of the database.

(b) How is access to data in the system determined?

Access is approved by the supervisor and the local Information System Security Officer (ISSO). Access is role-based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

Information and procedures are documented in the eDP System Security Plan

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Users other than the eDP manager and administrators will not have access to all functions involving data in the system. Users can view all data; however, there are restrictions regarding what data each user can change or update based on their roles. Separation of duties and least privilege is employed. Users will have access to only the data that the supervisor and the local ISSO approve to perform official duties. The four primary eDP system users are as follows:

eDP Post Consular Officers/users: eDP has functions performed by individuals in three roles:
- eDP Manager: Has access to all functions and information i.e., search, scan, edit, attach documents, delete, view, print barcodes and images.
- eDP Data Entry: Has access to all functions and information with the exception of deleting documents.
- eDP Read only: Has access to read all information, but can only search cases, restore documents and drag and drop files.

eDP Web users: eDP Web can be accessed by only those users who have access to the Consular Consolidated Database (CCD) and have CCD roles. Most eDP Web users can read all information and only perform searches. The only user role in eDP Web that can see and alter content is the IVO Foreign Service Officer (FSO). The IVO FSO is able to mark an electronic document as "Original Seen and Compared" after comparing it with original documents obtained during a post interview.

System Administrators: System Administrators have access to all information and are responsible for daily maintenance, establishing access control lists (ACLs), and backups.

Database Administrators: Database Administrators (DBA) have access to all information and are responsible for daily maintenance, upgrades, patch/hot fixes, backups and configuration of the database. DBA access is controlled by the Data Engineering (DE) team through the use of access control lists.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

- Access control policies and access enforcement mechanisms control access to PII in eDP.

- Separation of duties is implemented; access is role based as required by policy.

- Least Privileges in eDP are restrictive rights/privileges or accesses by users for performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- Users are uniquely identified and authenticated before accessing PII in the eDP system.

In addition to the restrictions mentioned above in section 9d, all accounts are subject to automatic auditing.